Chapter 5

Automorphisms and bases

10 Automorphisms

In this chapter, we will once again adopt the viewpoint that a finite extension $F = \mathbb{F}_{q^m}$ of a finite field $K = \mathbb{F}_q$ is a vector space of dimension m over K.

In Theorem 7.3 we saw that the set of roots of an irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree m is the set of m distinct elements $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}$ of $\mathbb{F}_{q^m}$.

Definition 10.1
Let $\mathbb{F}_{q^m}$ be an extension of $\mathbb{F}_q$ and let $\alpha \in \mathbb{F}_{q^m}$. The elements $\alpha, \alpha^q, \dots, \alpha^{q^{m-1}}$ are called the *conjugates* of α with respect to $\mathbb{F}_q$.

Remark 10.2

- *The conjugates of $\alpha \in \mathbb{F}_{q^m}$ with respect to $\mathbb{F}_q$ are distinct if and only if the minimal polynomial g of α over $\mathbb{F}_q$ has degree m.*
- *Otherwise, the degree d of the minimal polynomial g of α over $\mathbb{F}_q$ is a proper divisor of m, and in this case the conjugates of α with respect to $\mathbb{F}_q$ are the distinct elements $\alpha, \alpha^q, \dots, \alpha^{q^{d-1}}$, each repeated m/d times.*

Theorem 10.3
The conjugates of $\alpha \in \mathbb{F}_q^*$ with respect to any subfield of $\mathbb{F}_q$ have the same order in the group $\mathbb{F}_q^*$.

Proof. Apply Theorem 1.13 to the cyclic group $\mathbb{F}_q^*$, using the fact that every power of the characteristic of $\mathbb{F}_q$ is coprime to the order $q-1$ of $\mathbb{F}_q^*$. ■

This immediately implies the following observation.

Corollary 10.4
If α is a primitive element of $\mathbb{F}_{q^m}$, then so are all its conjugates with respect to $\mathbb{F}_q$.

Example 10.5
Expressing $\mathbb{F}_4$ as $\mathbb{F}_2(\theta) = \{0, 1, \theta, \theta+1\}$, where $\theta^2 + \theta + 1 = 0$, we saw in Example 6.11 that θ is a primitive element of $\mathbb{F}_4$. The conjugates of $\theta \in \mathbb{F}_4$ with respect to $\mathbb{F}_2$ are θ and θ^2; from Example 6.11, $\theta^2 = \theta + 1$ is also a primitive element.

Example 10.6
Let $\alpha \in \mathbb{F}_{16}$ be a root of $f = x^4 + x + 1 \in \mathbb{F}_2[x]$. Then the conjugates of α with respect to $\mathbb{F}_2$ are $\alpha, \alpha^2, \alpha^4 = \alpha + 1, \alpha^8 = \alpha^2 + 1$, and all of these are primitive elements of $\mathbb{F}_{16}$. The conjugates of α with respect to $\mathbb{F}_4$ are α and $\alpha^4 = \alpha + 1$.

We next explore the relationship between conjugate elements and certain automorphisms of a finite field.

Definition 10.7
An *automorphism of* $\mathbb{F}_{q^m}$ *over* $\mathbb{F}_q$ is an automorphism σ of $\mathbb{F}_{q^m}$ which fixes the elements of $\mathbb{F}_q$ pointwise. Thus, σ is a one-to-one mapping from $\mathbb{F}_{q^m}$ onto itself with

$$\sigma(\alpha+\beta) = \sigma(\alpha) + \sigma(\beta)$$

and

$$\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$$

for all $\alpha, \beta \in \mathbb{F}_{q^m}$ and

$$\sigma(a) = a \text{ for all } a \in \mathbb{F}_q.$$

This definition may look familiar to anyone who has studied Galois theory!

Theorem 10.8
The distinct automorphisms of $\mathbb{F}_{q^m}$ *over* $\mathbb{F}_q$ *are precisely the mappings* $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$ *defined by*

$$\sigma_j(\alpha) = \alpha^{q^j}$$

for $\alpha \in \mathbb{F}_{q^m}$ *and* $0 \le j \le m-1$.

Proof. We first establish that the mappings σ_j are automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

- For each σ_j and all $\alpha, \beta \in \mathbb{F}_{q^m}$, we have $\sigma_j(\alpha\beta) = \sigma_j(\alpha)\sigma_j(\beta)$ and $\sigma_j(\alpha+\beta) = \sigma_j(\alpha) + \sigma_j(\beta)$ by Freshmen's Exponentiation, so clearly σ_j is an endomorphism of $\mathbb{F}_{q^m}$.
- Since $\sigma_j(\alpha) = 0 \Leftrightarrow \alpha = 0$, σ_j is injective. Since $\mathbb{F}_{q^m}$ is a finite set, σ_j is also surjective, and hence is an automorphism of $\mathbb{F}_{q^m}$.
- We have $\sigma_j(a) = a$ for all $a \in \mathbb{F}_q$ by Lemma 6.3, and so each σ_j is an automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.
- The mappings $\sigma_1, \ldots, \sigma_{m-1}$ are distinct as they return distinct values for a primitive element of $\mathbb{F}_{q^m}$.

Now, suppose σ is an arbitrary automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$; we show that it is in fact σ_j for some $0 \le j \le m-1$.

Let β be a primitive element of $\mathbb{F}_{q^m}$ and let $f = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in \mathbb{F}_q[x]$ be its minimal polynomial over $\mathbb{F}_q$. Then

$$\begin{aligned} 0 &= \sigma(\beta^m + a_{m-}\beta^{m-1} + \cdots + a_0) \\ &= \sigma(\beta)^m + a_{m-1}\sigma(\beta)^{m-1} + \cdots + a_0, \end{aligned}$$

so that $\sigma(\beta)$ is a root of f in $\mathbb{F}_{q^m}$. By Theorem 7.3, we must have $\sigma(\beta) = \beta^{q^j}$ for some j, $0 \le j \le m-1$. Since σ is a homomorphism and β primitive, we get that $\sigma(\alpha) = \alpha^{q^j}$ for all $\alpha \in \mathbb{F}_{q^m}$. ■

Hence the conjugates of $\alpha \in \mathbb{F}_{q^m}$ are obtained by applying all automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ to the element α.

Remark 10.9
The automorphisms of $\mathbb{F}_{q^m}$ *over* $\mathbb{F}_q$ *form a group under composition of mappings, called the* Galois group *of* $\mathbb{F}_{q^m}$ *over* $\mathbb{F}_q$ *and denoted* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. *From Theorem 10.8, this group of automorphisms is a cyclic group of order* m*, generated by* σ_1.

11 Traces and Norms

Let $F = \mathbb{F}_{q^m}$ and $K = \mathbb{F}_q$. We introduce a mapping from F to K which turns out to be K-linear.

Definition 11.1
For $\alpha \in F$, the *trace* $\mathrm{Tr}_{F/K}(\alpha)$ of α over K is defined by

$$\begin{aligned} \mathrm{Tr}_{F/K}(\alpha) &= \text{sum of conjugates of } \alpha \text{ w.r.t. } K \\ &= \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}} \end{aligned}$$

If K is the prime subfield of F, i.e. $K = \mathbb{F}_p$ where p is the characteristic of F, then $\mathrm{Tr}_{F/K}(\alpha)$ is called the absolute trace of α and denoted simply by $\mathrm{Tr}(\alpha)$.

A useful alternative way to think of the trace is as follows.

Definition 11.2
Let $\alpha \in F$ and $f \in K[x]$ be the minimal polynomial of α over K; its degree d is a divisor of $m = [F : K]$. Then $g = f^{m/d} \in K[x]$ is called the *characteristic polynomial* of α over K.

By Theorem 7.3, the roots of f in F are $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$; from Remark 10.2, the roots of g in F are precisely the conjugates of α with respect to K. So

$$\begin{aligned} g &= x^m + a_{m-1}x^{m-1} + \cdots + a_0 \\ &= (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{m-1}}). \end{aligned}$$

Comparing coefficients we see that

$$\mathrm{Tr}_{F/K}(\alpha) = -a_{m-1}.$$

In particular, $\mathrm{Tr}_{F/K}(\alpha)$ must be an element of K.

Theorem 11.3
Let $K = \mathbb{F}_q$ and let $F = \mathbb{F}_{q^m}$. Then the trace function $\mathrm{Tr}_{F/K}$ satisfies the following properties.

(i) $\mathrm{Tr}_{F/K}(\alpha+\beta) = \mathrm{Tr}_{F/K}(\alpha) + \mathrm{Tr}_{F/K}(\beta)$ *for all* $\alpha, \beta \in F$*;*

(ii) $\mathrm{Tr}_{F/K}(c\alpha) = c\mathrm{Tr}_{F/K}(\alpha)$ *for all* $c \in K$*,* $\alpha \in F$*;*

(iii) $\mathrm{Tr}_{F/K}$ *is a linear transformation from* F *onto* K *(both viewed as* K *vector spaces);*

(iv) $\mathrm{Tr}_{F/K}(a) = ma$ *for all* $a \in K$*;*

(v) $\mathrm{Tr}_{F/K}(\alpha^q) = \mathrm{Tr}_{F/K}(\alpha)$ *for all* $\alpha \in F$*.*

Proof. (i) For $\alpha, \beta \in F$, Freshmen's Exponentiation yields

$$\begin{aligned} \mathrm{Tr}_{F/K}(\alpha+\beta) &= \alpha + \beta + (\alpha+\beta)^q + \cdots + (\alpha+\beta)^{q^{m-1}} \\ &= \alpha + \beta + \alpha^q + \beta^q + \cdots + \alpha^{q^{m-1}} + \beta^{q^{m-1}} \\ &= \mathrm{Tr}_{F/K}(\alpha) + \mathrm{Tr}_{F/K}(\beta). \end{aligned}$$

(ii) By Lemma 6.3, for $c \in K$ we have $c^{q^i} = c$ for all $i \geq 0$. Then for $\alpha \in F$,

$$\begin{aligned} \mathrm{Tr}_{F/K}(c\alpha) &= c\alpha + c^q\alpha^q + \cdots + c^{q^{m-1}}\alpha^{q^{m-1}} \\ &= c\alpha + c\alpha^q + \cdots + c\alpha^{q^{m-1}} \\ &= c\mathrm{Tr}_{F/K}(\alpha). \end{aligned}$$

(iii) For all $\alpha \in F$ we have $\mathrm{Tr}_{F/K}(\alpha) \in K$; this follows from the discussion above, or immediately from

$$\begin{aligned}(\mathrm{Tr}_{F/K}(\alpha))^q &= (\alpha + \alpha^q + \cdots + \alpha^{q^{m-1}})^q \\ &= \alpha^q + \cdots + \alpha^{q^{m-1}} + \alpha \\ &= \mathrm{Tr}_{F/K}(\alpha).\end{aligned}$$

Combining this with (i) and (ii) shows that $\mathrm{Tr}_{F/K}$ is a K-linear transformation from F into K. To show that it is surjective, it suffices to demonstrate that there exists some $\alpha \in F$ with $\mathrm{Tr}_{F/K}(\alpha) \neq 0$. We have $\mathrm{Tr}_{F/K}(\alpha) = 0 \Leftrightarrow \alpha$ is a root of $x^{q^{m-1}} + \cdots + x^q + x \in K[x]$ in F; since this polynomial has at most q^{m-1} roots in F whereas F has q^m elements, the result follows.
(iv) By Lemma 7.3, $a^{q^i} = a$ for all $a \in K$ and $i \geq 0$, and the result follows.
(v) For $\alpha \in F$ we have $\alpha^{q^m} = \alpha$, and so

$$\mathrm{Tr}_{F/K}(\alpha^q) = \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^m} = \mathrm{Tr}_{F/K}(\alpha).$$

■

In fact, the trace function provides a description for all linear transformations from F into K, in the following sense.

Theorem 11.4
Let F be a finite extension of the finite field K (both viewed as vector spaces over K). Then the K-linear transformations from F into K are precisely the mappings L_β ($\beta \in F$) given by $L_\beta(\alpha) = \mathrm{Tr}_{F/K}(\beta\alpha)$ for all $\alpha \in F$. Moreover, if α, β are distinct elements of F then $L_\alpha \neq L_\beta$.

Proof. Omitted. Idea: $(\alpha, \beta) \mapsto \mathrm{Tr}_{F/K}(\alpha\beta)$ is a symmetric non-degenerate bilinear form on the K-vectorspace F. ■

For a chain of extensions, we have the following rule.

Theorem 11.5 (Transitivity of trace)
Let K be a finite field, let F be a finite extension of K and E a finite extension of F. Then

$$\mathrm{Tr}_{E/K}(\alpha) = \mathrm{Tr}_{F/K}(\mathrm{Tr}_{E/F}(\alpha))$$

for all $\alpha \in E$.

Proof. Let $K = \mathbb{F}_q$, let $[F : K] = m$ and let $[E : F] = n$, so that $[E : K] = mn$ by Theorem 5.6. For $\alpha \in E$,

$$\begin{aligned}\mathrm{Tr}_{F/K}(\mathrm{Tr}_{E/F}(\alpha)) &= \sum_{i=0}^{m-1} \mathrm{Tr}_{F/K}(\alpha)^{q^i} \\ &= \sum_{i=0}^{m-1} (\sum_{j=0}^{n-1} \alpha^{q^{jm}})^{q^i} \\ &= \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \alpha^{q^{jm+i}} \\ &= \sum_{k=0}^{mn-1} \alpha^{q^k} = \mathrm{Tr}_{E/K}(\alpha).\end{aligned}$$

■

The multiplicative analogue of the trace function is called the norm.

Definition 11.6
For $\alpha \in F = \mathbb{F}_{q^m}$ and $K = \mathbb{F}_q$, the *norm* $N_{F/K}(\alpha)$ of α over K is defined by

$$\begin{aligned} N_{F/K}(\alpha) &= \text{product of conjugates of } \alpha \text{ w.r.t. } K \\ &= \alpha \cdot \alpha^q \cdots \alpha^{q^{m-1}} \\ &= \alpha^{(q^m-1)/(q-1)}. \end{aligned}$$

Comparing this definition with the characteristic polynomial g of α over K, as before, we see that

$$N_{F/K}(\alpha) = (-1)^m a_0.$$

In particular, $N_{F/K}(\alpha)$ is always an element of K.

Theorem 11.7
Let $K = \mathbb{F}_q$, and F its degree m extension. The norm function $N_{F/K}$ satisfies the following properties:

(i) $N_{F/K}(\alpha\beta) = N_{F/K}(\alpha)N_{F/K}(\beta)$ *for all* $\alpha, \beta \in F$*;*

(ii) $N_{F/K}$ *maps* F *onto* K *and* F^* *onto* K^**;*

(iii) $N_{F/K}(a) = a^m$ *for all* $a \in K$*;*

(iv) $N_{F/K}(\alpha^q) = N_{F/K}(\alpha)$ *for all* $\alpha \in F$*.*

Proof. (i) Immediate from definition of norm.
(ii) From above, $N_{F/K}$ maps F into K; since $N_{F/K}(\alpha) = 0 \Leftrightarrow \alpha = 0$, we have that $N_{F/K}$ maps F^* into K^*.

We must now show that $N_{F/K}$ is surjective. By (i), $N_{F/K}$ is a homomorphism between the multiplicative groups F^* and K^*. The elements of the kernel are the roots of $x^{\frac{q^m-1}{q-1}} - 1 \in K[x]$ in F; denoting the order of the kernel by d, we have $d \leq \frac{q^m-1}{q-1}$. By the First Isomorphism Theorem, the image has order $(q^m-1)/d$, which is at least $q-1$. So $N_{F/K}$ maps F^* onto K^* and hence F onto K.
(iii) Result is immediate upon noting that, for $a \in K$, all conjugates of a are equal to a.
(iv) By (i), $N_{F/K}(\alpha^q) = N_{F/K}(\alpha)^q$; by (ii), $N_{F/K}(\alpha) \in K$ and so $N_{F/K}(\alpha)^q = N_{F/K}(\alpha)$. ■

Theorem 11.8 (Transitivity of Norm)
Let K be a finite field, let F be a finite extension of K and let E be a finite extension of F. Then

$$N_{E/K}(\alpha) = N_{F/K}(N_{E/F}(\alpha))$$

for all $\alpha \in E$*.*

Proof. Let $[F : K] = m$ and $[E : F] = n$. Then for $\alpha \in E$,

$$\begin{aligned} N_{F/K}(N_{E/F}(\alpha)) &= N_{F/K}\left(\alpha^{\frac{q^{mn}-1}{q^m-1}}\right) \\ &= \left(\alpha^{\frac{q^{mn}-1}{q^m-1}}\right)^{\frac{q^m-1}{q-1}} \\ &= \alpha^{\frac{q^{mn}-1}{q-1}} = N_{E/K}(\alpha). \end{aligned}$$

■

12 Bases and the Normal Basis Theorem

We first consider two important, and very natural, kinds of bases.

Recall that $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha) \cong \mathbb{F}_q[x]/(f)$, where f is an irreducible polynomial of degree m and α is a root of f in $\mathbb{F}_{q^m}$. So, every element of $\mathbb{F}_{q^m}$ can be uniquely expressed as a polynomial in α over $\mathbb{F}_q$ of degree less than m and hence, for any defining element α, the set $\{1, \alpha, \ldots, \alpha^{m-1}\}$ is a basis for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

Definition 12.1
Let $K = \mathbb{F}_q$ and $F = \mathbb{F}_{q^m}$.

A *polynomial basis* of F over K is a basis of the form $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$, where α is a defining element of F over K.

We can always insist that the element α is a primitive element of F, since by Theorem 6.12, every primitive element of F can serve as a defining element of F over K.

Example 12.2
Let $K = \mathbb{F}_3$ and $F = \mathbb{F}_9$. Then F is a simple algebraic extension of K of degree 2, obtained by adjoining an appropriate θ to K. Let θ be a root of the irreducible polynomial $x^2 + 1 \in K[x]$; then $\{1, \theta\}$ is a polynomial basis for F over K. However, θ is not primitive since $\theta^4 = 1$. Now let α be a root of $x^2 + x + 2$; then $\{1, \alpha\}$ is another polynomial basis for F over K, and α is a primitive element of F.

Definition 12.3
Let $K = \mathbb{F}_q$ and $F = \mathbb{F}_{q^m}$. A *normal basis* of F over K is a basis of the form $\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$, consisting of a suitable element $\alpha \in F$ and all its conjugates with respect to K. Such an α is called a *free* or *normal* element.

Example 12.4
Let $K = \mathbb{F}_2$ and $F = \mathbb{F}_8$. Let $\alpha \in \mathbb{F}_8$ be a root of the irreducible polynomial $x^3 + x^2 + 1$ in $\mathbb{F}_2[x]$. Then $B = \{\alpha, \alpha^2, 1 + \alpha + \alpha^2\}$ is a basis of $\mathbb{F}_8$ over $\mathbb{F}_2$. Since $\alpha^4 = 1 + \alpha + \alpha^2$, this is in fact a normal basis for F over K. To the contrary, let $\beta \in F$ be a root of the irreducible polynomial $x^3 + x + 1 \in K[x]$. Then the conjugates $\{\beta, \beta^2, \beta^2 + \beta\}$ of β do not form a basis of K.

We now ask: does a normal basis exist for every F and K?
We require two lemmas before proving the main result.

Lemma 12.5 (Artin Lemma)
Let $\chi_1, \ldots, \chi_m$ be distinct homomorphisms from a group G into the multiplicative group F^* of an arbitrary field F, and let $a_1, \ldots, a_m \in F$, not all zero. Then for some $g \in G$ we have

$$a_1\chi_1(g) + \ldots + a_m\chi_m(g) \neq 0.$$

Proof. The proof is by induction on m. We omit the details. ■

Next, we recall a few concepts from linear algebra.

Definition 12.6

- If T is a linear operator on a finite dimensional vector space V over an arbitrary field K, then a polynomial $f = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$ is said to *annihilate* T if $a_n T^n + \cdots + a_1 T + a_0 I = 0$, where I and 0 are the identity and zero operator on V, respectively.
- The uniquely determined monic polynomial of least degree with this property is called the *minimal polynomial* for T. It divides any other polynomial in $K[x]$ which annihilates T.

- The *characteristic polynomial* g for T is given by $g := \det(xI - T)$. It is a monic polynomial of degree $n = \dim(V)$; by the Cayley-Hamilton theorem it annihilates T (and hence is divisible by the minimal polynomial). In fact, the roots of the two polynomials are the same up to multiplicity.
- A vector $\alpha \in V$ is called a *cyclic vector* for T if the vectors $T^k\alpha$, $k = 0, 1, \ldots$ span V.

We are now ready for the second lemma.

Lemma 12.7
Let T be a linear operator on the finite-dimensional vector space V. Then T has a cyclic vector if and only if the characteristic and minimal polynomials for T are identical.

Proof. Omitted. ■

Theorem 12.8 (Normal Basis Theorem)
For any finite field K and any finite extension F of K, there exists a normal basis of F over K.

Proof. Let $K = \mathbb{F}_q$ and $F = \mathbb{F}_{q^m}$ with $m \geq 2$.

- From Theorem 10.8, the distinct automorphisms of F over K are given by

$$\epsilon, \sigma, \sigma^2, \ldots, \sigma^{m-1},$$

  where ϵ is the identity map on F, $\sigma(\alpha) = \alpha^q$ for $\alpha \in F$ and σ^i means composing σ with itself i times.
- Since $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ and $\sigma(c\alpha) = c\sigma(\alpha)$ for $\alpha, \beta \in F$ and $c \in K$, we can think of σ as a linear operator on the vector space F over K.
- Since $\sigma^m = \epsilon$, the polynomial $x^m - 1 \in K[x]$ annihilates σ. Consider $\epsilon, \sigma, \sigma^2, \ldots, \sigma^{m-1}$ as endomorphisms of F^*, and apply the Artin Lemma; this tells us that no nonzero polynomial in $K[x]$ of degree less than m annihilates σ. Thus, $x^m - 1$ is the minimal polynomial for the linear operator σ.
- Since the characteristic polynomial for σ is a monic polynomial of degree m divisible by the minimal polynomial for σ, we must have that $x^m - 1$ is the characteristic polynomial also.
- By Lemma 12.7, there must exist a cyclic vector for V; i.e. there exists some $\alpha \in F$ such that $\alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots$ span F.
- Dropping repeated elements, this says that $\alpha, \sigma(\alpha), \ldots, \sigma^{m-1}(\alpha)$ span F, and hence form a basis of F over K. Since this basis consists of an element and its conjugates with respect to K, it is a normal basis, as required!

■

In fact, it turns out that this result can be strengthened, in the following way.

Theorem 12.9 (Primitive Normal Basis Theorem)
For any finite extension F of a finite field K, there exists a normal basis of F over K that consists of primitive elements of F.

Proof. Beyond the scope of this course! ■

Example 12.10
Let $K = \mathbb{F}_2$ and $F = \mathbb{F}_8 = K(\alpha)$, where $\alpha^3 + \alpha^2 + 1 = 0$. We saw in Example 12.4 that the basis $B = \{\alpha, \alpha^2, 1 + \alpha + \alpha^2 = \alpha^4\}$ from Example 12.4 is a normal basis for F over K. In fact, α is a primitive element of F (F^* is the cyclic group of order 7 and hence any non-identity element is a generator). So this is a primitive normal basis for F over K.